DOI: 10.7251/JTTTP2502121K
UDC: 004.7.056.6:629.3.064

REVIEW SCIENTIFIC PAPER

Cyber attacks on autonomous vehicles in the VANET computer network (attacks and protection)

Boris Kovačić
Pan-European University APEIRON Banja Luka

Zoran Ž. Avramović
University of Belgrade, Pan-European University APEIRON Banja Luka

Ivana Buzdovan
University of Adriatic Bar, Montenegro

Received: December 1, 2025
Accepted: December 12, 2025

Abstract: Autonomous vehicles represent a revolution in mobility, but they raise the issue of security challenges. With their appearance and the introduction of the 5G network, traffic systems are becoming increasingly dependent on digital communication and real-time data processing. Connectivity through 5G networks and ad-hoc communication protocols makes them vulnerable to various forms of cyber attacks, which can threaten lives, property and public safety. The paper analyzes the threats to which autonomous vehicles are exposed within the VANET network (a specialized class of ad-hoc networks in which vehicles function as nodes in the communication network) in a 5G environment. The consequences of an attack can be: complete disabling of the operation of one or more vehicles in the system, traffic accidents due to false data or errors in algorithms, compromising the privacy of passengers and vehicle owners, disruption of traffic infrastructure, as well as loss of public trust. Special emphasis in the paper is placed on the consequences for traffic safety and potential protection measures.

Key words: autonomous vehicles, cyber attack, VANET computer network, 5G network, IEEE standards, communications: V2V, V2I i V2X.

INTRODUCTION

An autonomous vehicle is said to be a vehicle that moves from one point to another without human intervention. Autonomy is achieved by installing well-placed sensors that detect various objects such as obstacles on the road, pedestrians, traffic lights, stopping and movement of other vehicles.

Autonomous vehicles represent not only the future, but also the present on the roads around us. As with conventional vehicles, the safety of the passengers in the vehicle, as well as other road users, must come first. Autonomous vehicles are expected to make an even greater contribution to traffic safety, which is an important motive for their development. The systems that are currently installed in autonomous vehicles are not designed so that they can avoid obstacles on the road by maneuvering at the limit of the capabilities of the vehicle and the surface. For these purposes, a universal training ground based on ISO 3888-1 and ISO 3888-2 standards was adopted, which can be used to represent any situation in which there is an obstacle on the road in front of the vehicle that needs to be avoided. One of the solutions for drawing paths through the polygon is to use Bezier curves. (Stamenković, 2022)

The architecture of the autonomous vehicle is based on a hybrid solution. Architecture can be divided into three groups:

1. The perception level consists of a fusion of different sensors that collect information from the outside world using a suitable algorithm
2. The control software layer consists of vehicle control agents, route planner, navigator and driver. This level can also be called the level of thoughtfulness.
3. The physical level of the vehicle contains vehicle control controls, that is, more precisely, engine control, steering control, brake control and transmission control. The physical level of the vehicle can also be called the reactive layer.

VANET NETWORK ARCHITECTURE

The collection and processing of VANET network data can be divided into several levels, and all these levels together make up the network architecture itself. All data is stored and exchanged in the VANET Cloud architecture. The purpose of this architecture is to reduce errors that occur during data detection, delay and quality itself.

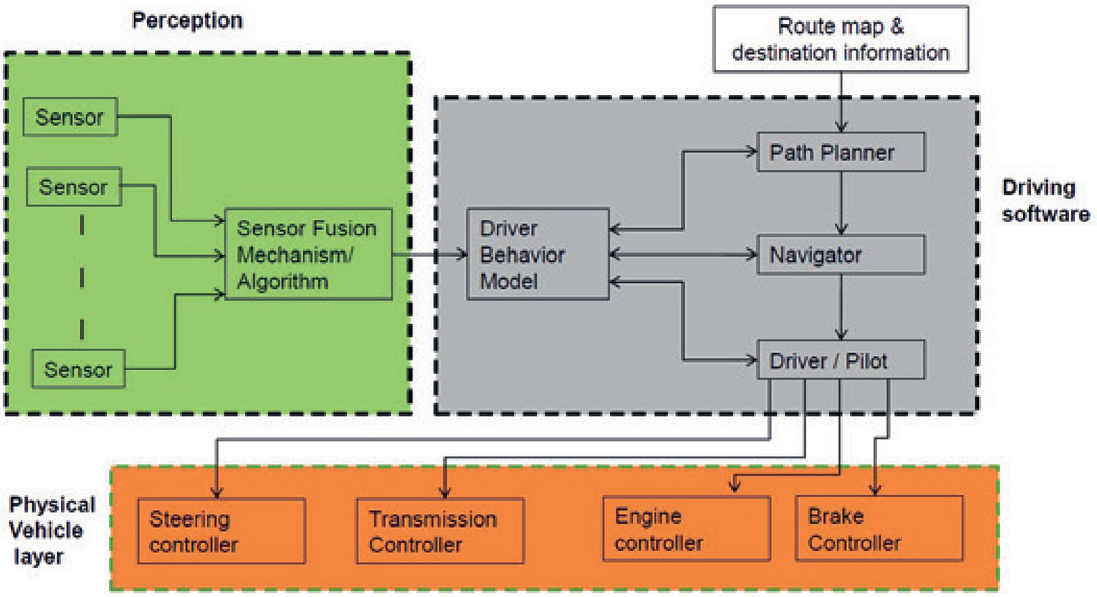

Figure 1. Sketch of autonomous vehicle architecture

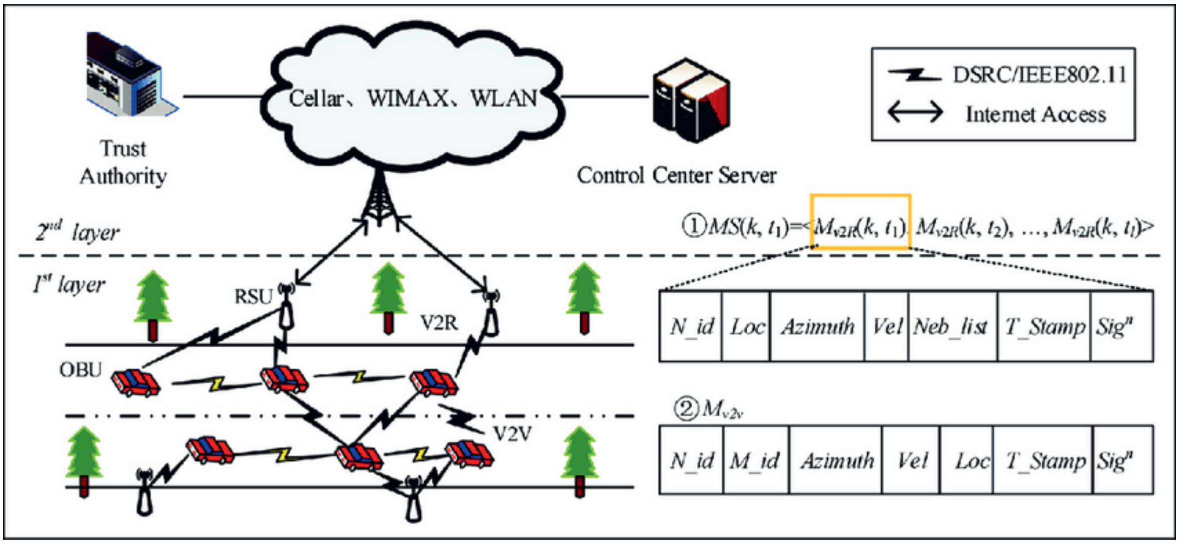

Figure 2. VANET network architecture (Xin, 2019)

There are three layers of architecture and they are: (Kovačević, 2020)

- *Traffic data collection layer*
- *Infrastructure as a service layer*
- *VANET Cloud layer*

Traffic data collection layer

This layer has the role of collecting data. All the data it processes and collects is obtained from the network itself. What is important to note is that the data it deals with must be processed in real time, i.e. almost instantaneously. Several parameters with which this layer works are: the speed of the vehicles themselves, the condition of the road and the traffic flow.

For the full operation of this layer of architecture, two interfaces are used, the communication interface, and the 'sensitive' data interface. The task of the sensitive data interface is to forward data to the Cloud. The communication interface is responsible for accessing traffic services in real time. Autonomous vehicles use 5G or higher network. It is preferable to have a network with the highest possible speed and the lowest possible latency.

Infrastructure as a service layer

The layer in which the infrastructure is used as a service has two sublayers, the physical resource sublayer and the virtualized sublayer. The physical resource sublayer groups the servers themselves depending on their characteristics. Servers are responsible for saving traffic data in real time. In addition, they allow access to various existing databases on traffic and road conditions.

VANET cloud layer

The VANET cloud layer, i.e. the cloud, is in charge of processing collected traffic data. After successfully processing all the data, the next step is to optimize the data prediction. Apart from predictions, it is important that the data sent to each vehicle is actually delivered to that vehicle and not to someone else. Predictive data in the cloud contains information such as travel time, traffic flow, speed, road closures and the like. (Ghoualmi-Zine, 2020)

The collection and processing of data is the center of this layer's work, and this is made possible by road-side detectors, RSU. RSU stands for Road Side Unit. The RSU passes such raw data to this layer using the UC 7420 device. It is a network device used to connect data collection devices and traffic lights using the UMTS network. The cloud offers two types of services. The first type of service is at the request of the user himself, and the second type of service is an automatic service. The on-demand service calculates data that is important to the user, such as travel plan planning and travel time. An automatic service is one that is essential for all road users, such as a traffic accident. Such events are sent to users themselves.

Data exchange in the VANET network

There are several models according to which messages are sent and received in a VANET network. Each model works in a different way, but they have in common that they provide a simple data exchange mechanism. There are three models of data exchange and they are:

- reactive data exchange,
- proactive data exchange and
- hybrid data exchange. (Kovačević, 2020)

Reactive exchange is based on protocols that work only when the user asks for some kind of information, therefore such protocols give better results. The main reactive protocol is AODV (Ad hoc on demand distance vector). Its task is to find a route to a destination, but only when that route is not known in advance. The working principle of this protocol is that each node within the network contains its own routing table. There are several pieces of information in that table, but the most important is information about arriving at the destination itself. In the event that a new, shorter route to the destination is discovered, AODV will save the new route and delete the old route.

Proactive data exchange is based on periodic updating of data, more precisely the routing table. The main protocol for this kind of exchange is the density-based routing protocol. The protocol itself ranks roads by density and arranges them in a hierarchy. This protocol works in real time. When it calculates the density on roads, it first sends a test packet, and only after that the route for the vehicle is selected.

Hybrid data exchange is based on an adaptive routing protocol, which is a combination of reactive and proactive. What this protocol takes into account is the speed and density of nodes. The density of nodes is calculated using LET (Link expiration time). If the nodes move at a high speed and their density is low, then the LET will be short, while conversely if the LET is relatively long, it means that the network is somewhat more static. The disadvantage of the adaptive routing protocol is that it uses a large number of periodic messages, which can lead to congestion.

Another type of protocol that exists are position-based protocols, the most famous of which is GSR (Geographic Source Protocol). As the name suggests, this protocol uses maps of cities and pulls information from them using RLS, reactive location service. Another positional protocol is GPSR (Greedy perimeter stateless routing) which has two modes of operation. One way is to forward the packets to the node that is geographically closest to it, and the other way is to forward the packets along a series of nodes. GPSR is unreliable and has high packet loss, so positioning protocols are not used in VANET networks.

Other protocols used by the VANET network are not mentioned in this paper, but only the most important ones.

EXAMPLES OF ATTACKS ON AUTONOMOUS VEHICLES:

Autonomous vehicles, which rely on artificial intelligence, sensors and wireless connectivity, represent a revolution in transportation — but also a new target for cyber attacks. Autonomous vehicles are vulnerable because they are connected to the Internet for navigation, communication with other vehicles and infrastructure. They use complex operating systems and firmware that may have security vulnerabilities. Cyber attacks can threaten the control of the vehicle, manipulate data or interfere with communication with other systems. The consequences that can be the result of a cyber attack are taking control of the vehicle, stealing personal data of passengers, disabling security systems, causing traffic accidents or traffic chaos.

In order to prevent the aforementioned cyber attacks, the industry works to improve cryptography and communication authentication, regularly improves and updates software, and issues system patches, introduces new and improves security protocols for V2V and V2I communication.

An attacker on an autonomous vehicle typically exploits a vulnerability in software, similar to an attack on a computer in a network. The steps it goes through during the attack are:

1. Target identification
2. System access
3. Taking control
4. Causing damage

Some examples of attacks are:

- In 2015, researchers Charlie Miller and Chris Valasek remotely hacked a Jeep Cherokee while it was driving, using a laptop and the Internet. They took control of the brakes, wipers, air conditioning and engine. The reaction of the manufacturer Fiat Chrysler is that it has recalled 1.4 million vehicles for safety upgrades.
- Ransomware attack on luxury vehicles in London in 2022, in which hackers stole 25 luxury cars using sophisticated hardware. With a targeted attack on contactless keys - by copying signals, vehicles are unlocked and started without a physical key.
- Cruise Company's Robotaxis vehicles in San Francisco 2022 clustered and stopped at an intersection, blocking traffic. Although the cause has not been officially confirmed, a hacker attack or software failure is suspected.
- Hackers managed to break into the software of the Stryker military vehicle. Hackers have managed to compromise the software of a US Army armored personnel carrier. Although a bullet can't penetrate it, a laptop can - which shows the vulnerability of even the most protected systems.
- Consumer Watchdog attack on Tesla vehicle in 2022 by non-profit group. The non-profit group managed to display the message "!Hacked!" on the screens of Tesla vehicles. The goal was to point out the vulnerability of the system and the need for better protection.

STANDARDS AND REGULATIONS

Manufacturers implement the "security by design" approach, which incorporates security requirements already in the development phase of each subsystem.

- Application of the ISO/SAE 21434 standard for engineering work on cyber security in vehicles.
- Complying with UNECE R 155 regulations on CSMS cyber security management system and R 156 on secure OTA software updates.
- Network segmentation within the vehicle to isolate infotainment systems from critical control units.

Regulation

- Manufacturers require from suppliers the application of ISO/SAE 21434 and regular audits of safety processes.
- They require the application of national regulations and directives, such as the EU NIS2, which contribute to the unique requirements for vehicle safety.

Communication protection and manufacturer's hardware solutions

The security of wireless interfaces and the CAN-bus network is essential for preventing unauthorized access.

- End-to-end encryption V2X (V2V, V2I) message.
- Using hardware modules for security key management (HSM) in ECU units.
- Two-factor authentication when accessing diagnostic ports.

SECURITY OF VANET NETWORKS

In VANET networks (Vehicular Ad Hoc Networks), attacks can be different and threaten the security, reliability and privacy of communication between vehicles and infrastructure. (Izet Jagodić, 2016) VANET networks are a special type of mobile ad hoc networks (MANET), where nodes are vehicles, and communication takes place at high speed in a dynamic environment. Attacks in VANET can be classified in several ways.

Types of attacks in VANET networks

1. By location of attack:

a) Attacks on vehicles (V2V):

- **Sybil Attack** – The attacker broadcasts multiple fake identities to create the illusion of a large number of vehicles nearby.
- **Bogus Information Attack** – Spreading false information (eg false information about a traffic accident).

b) Attacks on infrastructure (V2I):

- **Replay Attack** – Recording and resending messages to mislead the system.
- **Man-in-the-Middle (MitM)** – Interception and modification of communication between vehicle and RSU (Road Side Unit).

a) Attacks on vehicles (V2V):

Sybil Attack in VANET networks

Sybil Attack is a type of attack in which one attacking node (vehicle or device) simulates several different fake identities in the network. Instead of appearing as a single node, the attacker poses as multiple different vehicles, sending false information on behalf of each of these fictitious "nodes.".

Target of attack:

- Manipulation of network protocols that rely on the number of nodes or their location.
- Causing congestion, panic, or misdirecting vehicles.
- Undermining the reliability and security of the network.

Example in a VANET environment:

Imagine that there was a traffic accident in the tunnel. An attacker can create multiple Sybil identities and send messages like:

" Vehicle XY123 is located in front of the accident."
" Vehicle XY124 is also on site."
" Vehicle XY125 reports a huge crowd."

With enough messages like this, other participants in the network may think that the traffic accident is huge and decide to go the other way — which the attacker may want (eg to steal, avoid the police, or create chaos).

The consequences of a Sybil attack:

- False information in traffic (crowds, accidents, dangers)
- Violation of trust in the system
- Impeding the vehicle to make good decisions
- Potential accidents and economic damage

Sybil attack protection measures:

1. Authentication and certification of nodes:
   - ◊ Each vehicle receives a unique digital certificate from the authority.
   - ◊ Communication must be signed and verifiable.
2. Behavior detection:
   - ◊ If several nodes come from the same location and send similar messages → possible Sybil warning.
3. Trast- systems (***Trust Models***)**:**
   - ◊ Building trust based on the node's behavior history.
4. Location verification:
   - ◊ Comparing the reported location with GPS/RSU data. Sybil nodes usually have an identical physical location.
5. Limited number of identities per vehicle:
   - ◊ Identity issuing systems allow only one or a limited number of valid certificates per vehicle at the same time.

Bogus Information Attack in VANET networks

Bogus Information Attack represents the intentional sending of false or altered information in the traffic network with the aim of causing the wrong behavior of other vehicles or the entire network.

It is a form of active attack, because the attacker actively sends messages with false content.

Attacker's goals:

- Misinforming other vehicles in order to create confusion, congestion, or traffic incidents.
- Impact on navigation, routing, or driving decisions.
- Creating an advantage for oneself (eg shortening the journey by avoiding a crowd that one falsely reported).

Examples in a real scenario:

1. The attacker sends a message:

"Nikola Tesla Street is closed due to an accident - please avoid!"

- Although in reality there are no accidents. Other participants start using alternative routes → the attacker avoids the crowd.

2. The attacker claims:

" Traffic is completely free on the highway"

- Although the highway is actually congested. This can cause more traffic jams or even traffic accidents.

Consequences of the attack:

- Wrong route decisions made.
- Increased number of accidents or traffic jams.
- Reduced trust in the system.
- Potential economic losses and security threats.

Protection measures against Bogus Information Attack:

1. Authentication of the message source:
   - Only authorized vehicles with valid certificates can send information.
2. Cross-checking of messages:
   - Messages are verified through several independent nodes.
   - If only one node claims something and the others do not – the message can be marked as suspicious.
3. Location check:
   - Messages are checked based on GPS location and RSU units - if the vehicle claims to be somewhere, but is not physically there, the message is rejected.
4. History of node behavior:
   - If the node has already sent incorrect information several times → its "trust" decreases → the messages are ignored.
5. Digital signatures and encryption:
   - It guarantees the integrity of the message and the identity of the sender.

Table 1. The difference between Sybil and Bogus attacks

Characteristics	Sybil Attack	Bogus Information Attack
Identity number	More fakes	Usually one
The problem it causes	Fake node count	False information content
Goal	Manipulation of the network structure	Disinformation from other participants

b) Attacks on infrastructure (V2I):

Replay Attack

Replay Attack (rebroadcast attack) in VANET networks implies that the attacker intercepts a legitimate message, saves it, and then later re-broadcasts it into the network as if it were new and valid.

The goal of the attack is to mislead the system that the old information is still current, which can cause incorrect vehicle behavior, congestion, or security risks.

Example of how the attack is carried out

1. Vehicle A sends a valid message:

" Accident on the road ahead, avoid!"
(with real timestamp)

1. The attacker intercepts that message and saves it.
2. After some time (when the situation has already been resolved), the attacker re-broadcasts the same message to the network.
3. Other vehicles interpret that message as new and react - even though the information is outdated and incorrect.

Targets of attack:

- Creating a false perception of the situation (eg an accident that no longer exists).
- Causing unnecessary road avoidance, congestion or traffic jams.
- Trying to hide the real situation (broadcasting old safety reports instead of the current danger).
- Breaking the security protocol that relies on signed messages - because the original message is valid.

Consequences:

- Loss of confidence in the system.
- Wrong decisions about the route or behavior of the driver.
- Reduced efficiency of traffic regulation.
- Potential traffic accidents.

Protection against Replay Attack:

1. Timestamps:

◊ Each message contains the sending time.

◊ The receiver checks whether the message is “too old” and ignores it if it is.

2. Nonce and Sequence Number:

◊ Messages contain a non-repeating random number (nonce) or message number (sequence).

◊ A repeated message is easily detected as a duplicate.

3. Session Tokens / Session contexts:

◊ Each communication is tied to a session or time context.

◊ Old tokens are no longer valid.

4. Cryptographic protection (signatures and encryption):

◊ Signed messages with timestamp verification make this attack more difficult.

5. Smart RSU:

◊ If a previously seen message appears in the same area - it can be marked as suspicious.

Table 2. Key Difference Between Replay Attack and Bogus Attack

Attack	Description
Replay Attack	Resending a previously valid message to cause an incorrect reaction.
Bogus Attack	Sending new but fake messages with wrong information.

Man-in-the-Middle (MitM) Attack in VANET networks

Man-in-the-Middle (MitM) attack in VANET occurs when an attacker places himself between two communication nodes (e.g. between two vehicles or between a vehicle and infrastructure), intercepts the communication, and has the possibility to:

- eavesdrops on messages,
- edit message content,
- forwards modified messages as if coming from a legitimate source.

The goal is that other nodes do not notice that the communication is not direct.

The places where MitM occurs in VANET are:

1. V2V attacker changes messages about accidents, road conditions, etc.
2. The V2I attacker falsifies the data sent or received by the RSU.
3. V2X – attacks on GNSS (eg GPS), Wi-Fi, DSRC, 5G or other communication channels.

Example scenario:

Vehicle A sends a message to vehicle B:

„Danger – ice on the road ahead. “

The attacker intercepts that message, changes it to:

„The road is clear – no problems whatsoever. “

Vehicle B receives a false message → continues without caution → possible accident.

Attacker’s goals:

- Traffic diversion
- Spying on communication (eavesdropping)
- Entering false data into the network
- Disable authentication and trust

Consequences of a MitM attack:

- Violation of privacy
- Loss of data integrity
- The possibility of far-reaching sabotage
- Complete deformation of the traffic system in the area

MitM attack protection measures:

1. Traffic encryption

- All messages are sent via TLS/SSL or other encrypted channel.
- Even if the message is intercepted - the content remains unreadable.

2. Digital signatures

- Each message is cryptographically signed (eg using ECDSA).
- The recipient can verify authenticity and integrity.

3. Authentication with certificates

- Each communicating party must have a valid certificate from a CA (Certification Authority).
- Communication with unknown nodes is prevented.

4. Time-based verification and nonce value

- Timestamps and random values are used to avoid Replay + MitM attacks.

Table 3. Key Differences: MitM vs. Replay vs. Bogus

Characteristics	MitM Attack	Replay Attack	Bogus Info Attack
Type	Interception and modification	Resending an old message	Sending a new, fake message
Message control	Full (read, change, send)	Limited (playback only)	Full (generates from scratch)
Goal	Deception or espionage	Confusion, misinformation	Creating a false situation

5. Intrusion detection (IDS/IPS)

- Systems that monitor traffic anomalies (eg unusual number of messages or deviation in behavior).

2. By the nature of the attack:

a) Active attacks:

- **Denial of Service (DoS)** – Overloading a network or resource to prevent communication. (Aleksandra Kostić-Ljubisavljević, 2024)
- **Message Tampering** – Changing the content of messages in transit.
- **Jamming** – Jamming radio signals to prevent communication.

b) Passive attacks:

- **Eavesdropping** – Eavesdropping on communications to collect data.
- **Tracking** – Monitoring of vehicle movement through the analysis of communication data.

a) Active attacks:

Denial of Service (DoS) Attack in VANET networks

Denial of Service (DoS) Attack in VANET networks represents an attempt to prevent normal communication between vehicles or between vehicles and infrastructure, through network, resource or software overload.

The aim of the attack is to make the system unavailable to legitimate users - either short-term or permanently.

VANET systems depend on fast, reliable and low-latency communication. If an attacker sends a large number of useless requests or messages, he can:

- block the wireless channel (DSRC, 802.11p, LTE-V/5G),
- occupy processor and memory resources in vehicles or RSU units,
- disable the processing of important messages (e.g. about an accident or braking).

Table 4. Examples of DoS attacks in VANET

Type of DoS attack	Description
Flooding Attack	The attacker sends a huge number of messages and thus occupies the channel.
Jamming Attack	Radio frequency jamming – real "noise" that blocks communication.
Malformed Packets	Sending messages with errors that cause the recipient's system to crash.
Resource Exhaustion	Memory, processor or bandwidth overload.

Goals of DoS attackers:

- Prevent the timely exchange of traffic data.
- Slow down or disrupt navigation systems.
- Cause accidents or chaos in traffic.
- Distract security systems in order to perform another attack (e.g. MitM or Bogus Attack).

Consequences of a DoS attack:

- Interruptions in V2V/V2I communication.
- Unprocessed critical messages (e.g. emergency braking).
- Decline of network infrastructure (RSU, control centers).
- Loss of confidence in vehicle security systems.

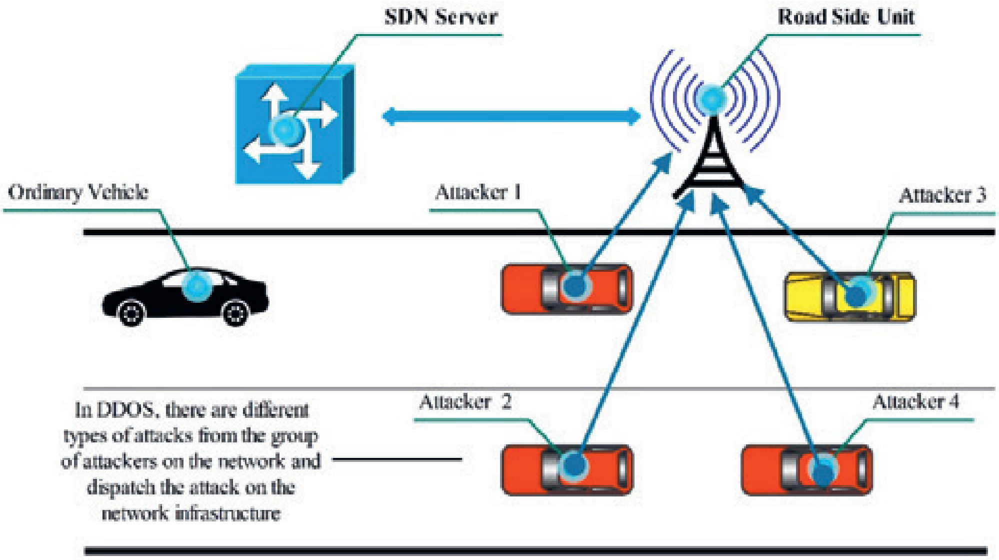
SDN Server
Road Side Unit
Ordinary Vehicle
Attacker 1
Attacker 3
Attacker 2
Attacker 4
In DDOS, there are different types of attacks from the group of attackers on the network and dispatch the attack on the network infrastructure

Figure 3. Example of a DDoS attack (Rashid, 2023)

Protection against DoS attacks:

1. Message rate limitation (Rate Limiting):
- RSUs and vehicles limit the number of messages they process from the same source in a certain time.

2. Detection of anomalies (Intrusion Detection Systems):
- Unusual number of messages, speed, packet size are monitored - suspicious patterns are detected.

3. Physical protection (Anti-Jamming):
- Using frequency hopping (Frequency Hopping), changeable channels and advanced antennas.

4. Filtering at the protocol level:
- Discard messages that do not respect the protocol (eg wrong length, incorrect headers).

5. Cryptographic protection:
- Although it does not prevent DoS directly, it prevents an attacker from broadcasting valid messages in large numbers without proper certificates.

Message Tampering Attack in VANET networks

Message Tampering is a type of attack in VANET networks in which the attacker modifies the content of a legitimate message in transit, before it reaches the recipient. The goal of the attack is to change the meaning or effect of the message without the knowledge of the original sender and receiver.

It is an active attack on data integrity, because the message appears as if it came from a legitimate source, but its content has been maliciously modified.

This type of attack occurs Between two vehicles (V2V), Between vehicle and infrastructure (V2I), Inside a malicious node that redirects messages, Combination with Man-in-the-Middle (MitM) attack

The vehicle receives incorrect information that the road is clear, even though it is ahead of accidents, which causes a possible collision.

Attacker's goals:

- Hiding or changing critical traffic information (eg accidents, roadblocks, weather conditions)
- Steering the vehicle in dangerous or wrong directions
- Creating chaos or bias in traffic (eg political or criminal intentions)
- Sabotaging communication or creating conditions for other attacks (eg DoS, Sybil, Bogus)

Consequences:

- Loss of data integrity
- Wrong driving decisions
- Injuries and accidents
- Loss of confidence in the VANET system

Protection against Message Tampering attacks:

1. Cryptographic digital signatures
- Each message is signed with the sender's private key.
- If the message is changed - the signature is no longer valid.
- Recipients can check whether the message is authentic and the integrity is preserved.

2. End-to-End encryption
- Messages are encrypted so that only the legitimate recipient can read or modify them.

3. Hash functions and MAC (Message Authentication Code)
- The message contains a hash value or MAC which is calculated based on the content and the key.
- Every message change changes the hash → easy to detect.

4. Timestamp and nonce verification
- A change to an old message (or its interception and modification) is detected if the time stamp is inconsistent.

5. Control via RSU and IDS system
- Messages are monitored and compared with other sources.
- If one message deviates from the majority, it is marked as suspicious.

In practice, the system receiving the messages must check the digital signature to detect this change.

Attacker's goals:

- Disabling vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication
- Preventing notifications about traffic accidents, conditions or emergency warnings
- Confusing autonomous vehicles
- Preparing the ground for other attacks (eg DoS, Sybil, MitM)

Consequences of Jamming attacks:

- Loss of all forms of communication (traffic, security, control)
- Increased risk of collision or traffic chaos
- Crash of the navigation and route planning system
- Disabling the operation of safety systems (ADAS, collision avoidance)

Protection against Jamming attacks:

1. Frequency Hopping Spread Spectrum (FHSS)
- Vehicles change communication frequency quickly → difficult for an attacker to follow

2. Direct Sequence Spread Spectrum (DSSS)
- The message spreads over a wide spectrum → better resistance to noise

3. Use of several channels (Multi-channel communication)
- Switching communication to less loaded channels

4. Detection on the physical layer
- Monitoring noise level, SNR (Signal-to-Noise Ratio), and other RF parameters
- Recognition of abnormal radio activity

5. Machine Learning IDS
- Using algorithms to recognize patterns that indicate interference

b) Passive attacks:

Eavesdropping attack in VANET networks

Eavesdropping is a passive attack in which an unauthorized attacker secretly eavesdrops on vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communications, with the aim of gathering sensitive or private information, without intercepting or altering messages.

The attacker remains invisible and only listens/records, often in preparation for more serious attacks like Man-in-the-Middle, Replay, or Bogus Information.

Eavesdropping in VANET occurs:
- Between two vehicles communicating via wireless channels (DSRC, IEEE 802.11p, LTE-V, 5G)
- Between RSU and vehicle
- Near traffic infrastructure (e.g. traffic lights, parking lots, pumps)

Example: What can the attacker get?
- Vehicle identifier (eg vehicle_id)
- Location and direction of movement
- Time and driving route
- Content of messages such as warnings, reported incidents
- Maybe even personal or financial information if encryption is not used

Attacker's goals:
- Espionage: tracking the movement of a specific vehicle (eg police, officials, important personalities)
- Gathering information: for planning other attacks (MitM, DoS)
- Driver profiling: habits, routes, frequency of road use
- Endangering the privacy and safety of road users

Consequences of Eavesdropping attacks:
- Violation of privacy
- Leakage of sensitive information
- Loss of trust in VANET network security
- Potential misuse for criminal activities (tracking, theft, sabotage)

Protection against Eavesdropping attacks:

1. Communication encryption (Encryption)
- Use symmetric or asymmetric encryption for all V2V and V2I messages (eg AES, RSA, ECC)
- DSRC and 5G-V2X already support cryptographic protection

2. Digital signatures
- Even if someone eavesdrops on the message, they cannot modify or reuse it

3. Vehicle anonymization (Pseudonymity)
- Vehicles change their identifiers at certain intervals to avoid tracking

4. Controlled range of transmission
- Limit the range of wireless signals → less chance that someone nearby can eavesdrop

5. Physical Layer Security (PHY-Sec)
- Techniques such as beamforming and channel-based keying → communication only between direct participants

Eavesdropping simulation in Python:

```
def eavesdrop(packet):
 print(f"[👂] Wiretapped message:")
 print(f" ID: {packet.get('vehicle_id')}")
 print(f" Location: {packet.get('location')}")
 print(f" Event: {packet.get('event')}")
 print(f" Time: {packet.get('timestamp')}")

# Example of a "captured" message
sample_packet = {
 "vehicle_id": "NS-987-XY",
 "location": {"latitude": 44.8000, "longitude": 20.4600},
 "event": "TRAFFIC_JAM",
 "timestamp": "2025-07-10T14:22:00Z"
}

eavesdrop(sample_packet)
```

In reality, such an attack would be performed using SDR (Software Defined Radio) devices such as HackRF or USRP, which can "listen" to the DSRC/5.9GHz band.

Tracking attack in VANET networks

A tracking attack in VANET is the misuse of communication data to track the movement of a specific vehicle or driver in space and time. This is a passive or semi-active attack that violates privacy, but can also have security implications.

The attacker uses information such as Vehicle ID, GPS coordinates, time and speed of movement from V2V/V2I messages to form a profile and route of movement of the target vehicle.

Goals of Tracking attackers:
- Track the route and habits (e.g. where the driver lives, works, stops)
- Monitoring of vehicles of interest (official, police, VIP)
- Warning when the vehicle enters a certain zone
- Commercial exploitation (advertisements, marketing, sale of data)
- Preparation for physical attacks, theft or sabotage

Consequences of Tracking attacks:
- Gross violation of privacy
- Physical danger for the driver
- Manipulation of data for extortion, blackmail or attack

- Loss of trust in the system

Protection against Tracking attacks:

1. Pseudonymization of IDs

- Instead of a permanent Vehicle ID, time-limited pseudonyms are used
- Change of pseudonym takes place at intervals or in "silent" zones

2. Silent periods

- Vehicles periodically stop broadcasting messages for a short time → difficult tracking

3. Group communication

- Messages are sent on behalf of a group of vehicles → difficult to attribute to a single node

4. Local encryption and masking

- Details such as location and timestamp can be masked or rounded

5. Mix Zones

Special zones in which several vehicles change pseudonyms synchronously → the connection between the old and new ID is lost

3. By target of attack:

a) Attacks on confidentiality:

- The goal is unauthorized access to data (eg personal data of the driver).

b) Attacks on integrity:

- Modification of messages so that their meaning changes (eg changes in traffic messages).

c) Attacks on availability:

- Preventing normal communication between participants in the network.

d) Attacks on authenticity:

- Falsification of the identity of a participant in the network (eg the vehicle is presented as a police vehicle).

PROTECTING AN AUTONOMOUS VEHICLE FROM CYBER ATTACKS WITH THE HELP OF JUMP SERVER

The problem that occurs in all the previously mentioned cases is cyber attacks on autonomous vehicles.

Autonomous vehicles use a multitude of sensors, software, networks (V2X), cloud services and ECU devices. This makes them a potential target for cyber attacks, such as:

- **Remote Code Execution** (RCE)
- **Unauthorized Access** (ECU hacking)
- **Manipulation of the AI system** (e.g. "data poisoning" or adversarial inputs)
- **GPS spoofing / sensor hijacking**
- **Denial-of-Service (DoS)** on critical control modules

These attacks can:

- Take complete control of the vehicle
- Disable communication
- Cause direct physical damage or accidents

Security solution using Jump Server as a security filter

Jump Server (or *Bastion Host*) is an intermediary server that must be passed through in order to access critical systems, such as ECUs, vehicle cloud services or communication channels.

In an autonomous vehicle, it is placed between:

- Internal vehicle systems (CAN, ECU, AI modules, V2X communication)
- And all external communication points (cloud, OTA update, V2I, service providers, etc.)

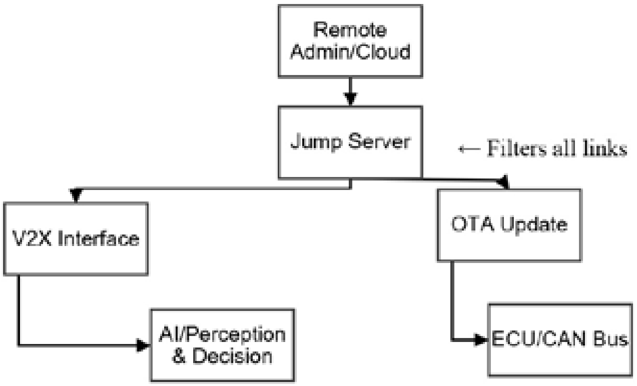

Figure 4. Protection architecture with Jump Server

Application in a real vehicle:

- Local (Edge): Jump server works in the vehicle itself as a "gateway firewall"
- Cloud-based OTA Access: Cloud must communicate through a centralized Jump server mechanism
- Servicer/Diagnostics: Must use time-limited tokens and access routes via Jump

The security policy provided by Jump Server:

- "Zero Trust": no one has direct access without verification
- "Least privilege": each access is limited by need
- "Audit everything": everything is logged and monitored

CONCLUSION

According to the above, it is clear that flawless cyber protection of autonomous vehicles is needed. The availability of access to autonomous vehicles through mesh networks and different communication channels complicates the cyber protection of vehicles. One of the solutions is the Jump server, as an innovative solution. Namely, the Jump server has been used in the protection of computer networks, primarily for channeling and protection of databases. It is mentioned as a possible solution in this paper, because in this way communication is channeled through one intermediary and in this way one point is defended. In addition, the progress of IoT devices, in terms of hardware, enables the use of better software solutions, such as Jump server.

In the future, the innovation that will be imposed in addition to the Jump server as a proposed solution for protection is a firewall, but a certain development of autonomous vehicles and sensors and IoT devices is required.

BIBLIOGRAPHY

[1] Aleksandra Kostić-Ljubisavljević, B. M. (2024). APPLICATION, ARCHITECTURES AND SECURITY OF SDN BASED VANET NETWORKS. *XLII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – PosTel 2024*, 138. Downloaded 11 15, 2025 from https://ebooks.sf.bg.ac.rs/index.php/1/catalog/view/24/36/756

[2] Ghoualmi-Zine, N. &. (2020). VANET: A novel service for predicting and disseminating vehicle traffic information. *International Journal of Communication Systems*. Downloaded from https://www.researchgate.net/publication/364070362_VANET_A_novel_service_for_predicting_and_disseminating_vehicle_traffic_information

[3] Izet Jagodić, S. K.-M. (2016). Sigurnosni uslovi i primjer aplikacije u mreži vozila. *INFOTEH-JAHORINA, 15*, 364. Downloaded 11 25, 2025 ca https://infoteh.etf.ues.rs.ba/zbornik/2016/radovi/KST-3/KST-3-6.pdf

[4] Kovačević, M. (2020). *KOMUNIKACIJA MEĐU VOZILIMA UNUTAR VANET.* Downloaded 11 25, 2025 ca https://repozitorij.etfos.hr/theses/etfos:2863/show-file/0

[5] Rashid, K. &. (2023). An Adaptive Real-Time Malicious Node Detection Framework Using Machine Learning in Vehicular Ad-Hoc Networks (VANETs). *Sensors, 23*. doi:10.3390/s23052594

[6] Stamenković, D. D. (2022). *Univerzitet u Beogradu Mašinski fakultet.* Downloaded 11 25, 2025 ca Model upravljanja autonomnim motornim vozilom, doktorska disertacija: https://nardus.mpn.gov.rs/bitstream/handle/123456789/22325/Disertacija_15219.pdf?sequence=1&isAllowed=y

[7] Xin, Y. &. (2019). Replica attack detection method for vehicular ad hoc networks with sequential trajectory segment. *International Journal of Distributed Sensor Networks*. doi:10.1177/1550147719827500